

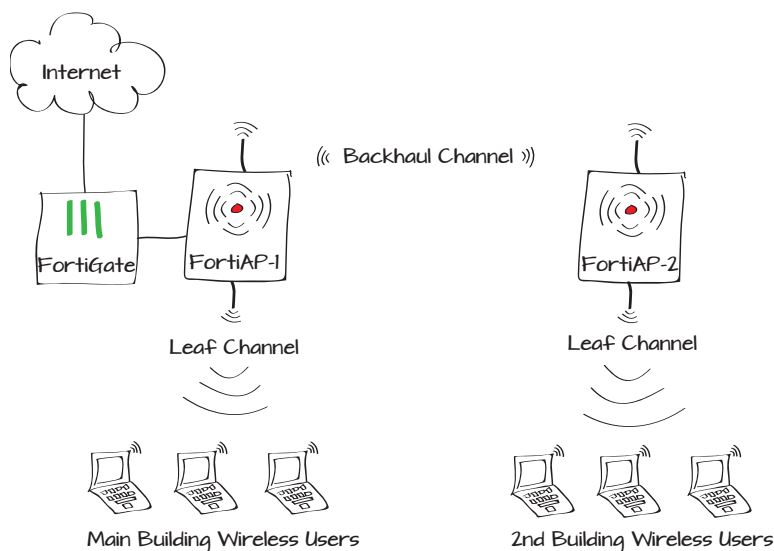
Extending the range of a wireless network by using mesh topology

This example demonstrates how to configure a FortiGate and two FortiAP wireless access point units to extend the reach and availability of a wireless network. This example simulates a company that has expanded into a second, nearby building that requires wireless access.



The FortiAP units used to create a wireless mesh must be models that have two radios.

1. Configuring an interface on the FortiGate for the APs
2. Creating two SSIDs
3. Creating a custom AP profile
4. Creating firewall addresses and an address group
5. Setting up and configuring the FortiAPs
6. Creating security policies on the FortiGate
7. Results



Before you begin

The following models were used in this example: FortiGate-100D, FortiAP-220B, and FortiAP-221B.

The FortiGate unit is in Interface Mode (each physical port can be the interface to a distinct subnet), so that a single port, in this case 11, will be used for the sole purpose of interface for the wireless network.

The computers managing the network and FortiAPs are located on the internal network.

Configuring an interface on the FortiGate for the APs

A dedicated network interface needs to be configured on the Fortigate that will be used only by the FortiAP units.

Go to **System > Network > Interfaces** and edit an available internal port (in the example, port11). Set **Addressing mode** to **Dedicate to FortiAP/FortiSwitch**.

Name	port11(00:09:0F:99:4B:F4)
Alias	FortiAP
Link Status	Up
Type	Physical Interface
Addressing mode <input type="radio"/> Manual <input type="radio"/> DHCP <input type="radio"/> PPPoE <input checked="" type="radio"/> Dedicate to FortiAP/FortiSwitch	
IP/Network Mask	192.168.11.1/255.255.255.0
1 Connected FortiAPs/FortiSwitches	
Device Management	
Detect and Identify Devices	<input type="checkbox"/>
Comments	<input type="text" value="Write a comment..."/> 0/255
Administrative Status	<input checked="" type="radio"/> Up <input type="radio"/> Down

Creating two SSIDs

A wireless mesh requires two SSIDs: back-haul and leaf. The backhaul channel is the wireless connection between the two FortiAP units, while the leaf channel is used by individual clients to connect to the wireless network.

Go to **System > Network > Interfaces** and create the backhaul SSID.

Set **Type** to **WiFi SSID** and configure the **WiFi Settings** as needed.

Create the leaf SSID.

Set **Type** to **WiFi SSID**, enable **DHCP Server**, and configure the **WiFi Settings** as needed.

Name	Backhaul.mesh
Type	WiFi SSID
Traffic Mode	Mesh Downlink

WiFi Settings

SSID	<input type="text" value="backhaul-ssid"/>
Security Mode	WPA/WPA2-Personal ▾
Data Encryption	<input checked="" type="radio"/> AES <input type="radio"/> TKIP <input type="radio"/> TKIP-AES
Pre-shared Key	<input type="password" value="••••••"/> (8 - 63 characters)

Name	leaf-ssid
Type	WiFi SSID
Traffic Mode	Tunnel to Wireless Controller

IP/Network Mask	192.168.205.1/255.255.255.0
IPv6 Address	:::0

Administrative Access	<input checked="" type="checkbox"/> HTTPS <input checked="" type="checkbox"/> PING <input checked="" type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access <input type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> TELNET <input type="checkbox"/> FCT-Access
IPv6 Administrative Access	<input type="checkbox"/> HTTPS <input type="checkbox"/> PING <input type="checkbox"/> HTTP <input type="checkbox"/> FMG-Access <input type="checkbox"/> SSH <input type="checkbox"/> SNMP <input type="checkbox"/> TELNET

DHCP Server	<input checked="" type="checkbox"/> Enable
-------------	--

Address Range	<div> Create New Edit Delete </div> <table border="1"> <thead> <tr> <th>Starting IP</th> <th>End IP</th> </tr> </thead> <tbody> <tr> <td>192.168.205.5</td> <td>192.168.205.254</td> </tr> </tbody> </table>	Starting IP	End IP	192.168.205.5	192.168.205.254
Starting IP	End IP				
192.168.205.5	192.168.205.254				
Netmask	255.255.255.0				
Default Gateway	<input checked="" type="radio"/> Same as Interface IP <input type="radio"/> Specify				
DNS Server	<input checked="" type="radio"/> Same as System DNS <input type="radio"/> Specify				
▶ Advanced...					

WiFi Settings	
SSID	leaf-ssid
Security Mode	WPA/WPA2-Personal
Data Encryption	<input checked="" type="radio"/> AES <input type="radio"/> TKIP <input type="radio"/> TKIP-AES
Pre-shared Key	<div> <div>•••••</div> <div>(8 - 63 characters)</div> </div>

Creating a custom AP profile

Go to **WiFi & Switch Controller > WiFi Network > Custom AP Profile**.

Create a new profile for the FortiAP model you are using.

Configure **Radio 1** for the backhaul channel and **Radio 2** for the leaf channel.

For the backhaul channel, set **Band** to **802.11an_5G**. For the leaf channel, set **Band** to **802.11bgn_2.4G**.



You may have to configure two custom AP profiles if your FortiAP units are different models that cannot use the same profile.

Radio 1

Mode: ☐ Disable ☒ Access Point ☐ Dedicated Monitor

Background Scan: ☒ Disable ☐ Enable

WIDS Profile:

Radio Resource Provision: ☒

Client Load Balancing: ☐ Frequency Handoff ☐ AP Handoff

Band:

20/40 MHz Channel Width: ☐

Channel: ☒ 36 ☒ 40 ☒ 44 ☒ 48 ☒ 149 ☒ 153 ☒ 157 ☒ 161 ☒ 165

Auto TX Power Control: ☒ Disable ☐ Enable

TX Power: 100 %

SSID

Available	Selected
leaf-ssid fortinet.mesh.root (Mesh S	backhaul-ssid (Mesh SSID

Radio 2

Mode: ☐ Disable ☒ Access Point ☐ Dedicated Monitor

Background Scan: ☒ Disable ☐ Enable

WIDS Profile:

Radio Resource Provision: ☒

Client Load Balancing: ☐ Frequency Handoff ☐ AP Handoff

Band:

Channel: ☒ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☒ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☒ 11

Auto TX Power Control: ☒ Disable ☐ Enable

TX Power: 100 %

SSID

Available	Selected
backhaul-ssid (Mesh SSID fortinet.mesh.root (Mesh S	leaf-ssid

Creating firewall addresses and an address group

Go to **Firewall Objects > Address > Addresses.**

Create a new address for the internal network.

Create an address for FortiAP-1.

Create an address for FortiAP-2.

Create an address for leaf channel users, using the DHCP range used by the leaf channel SSID.

Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

Internal_Network

Color

[Change]

Type

Subnet

Subnet / IP Range

192.168.150.0/255.255.255.0

Interface

LAN

Show in Address List

☒

Comments

Write a comment... 0/255

Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

FortiAP1

Color

[Change]

Type

Subnet

Subnet / IP Range

192.168.11.2

Interface

port11 (FortiAP)

Show in Address List

☒

Comments

Write a comment... 0/255

Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

FortiAP2

Color

[Change]

Type

Subnet

Subnet / IP Range

192.168.11.3

Interface

port11 (FortiAP)

Show in Address List

☒

Comments

Write a comment... 0/255

Category

☒ Address ☐ IPv6 Address ☐ Multicast Address

Name

Leaf_Wireless_Subnet

Color

[Change]

Type

Subnet

Subnet / IP Range

192.168.205.0/255.255.255.0

Interface

leaf-ssid (SSID: leaf-ssid)

Show in Address List

☒

Comments

Write a comment... 0/255

Go to **Firewall > Address > Groups** and create a new group.

Add the FortiAP addresses to the group.

Setting up and configuring the FortiAPs

In this example, the FortiAP-221B unit is FortiAP-1, while the FortiAP-220B is FortiAP-2.

Preauthorize FortiAP-1

Go to **WiFi & Switch Controller > Managed Devices > Managed FortiAP**. Select **Create New**.

Enter the serial number of the FortiAP unit and give the Managed Access Point a name.

Group Name	<input type="text" value="Mesh_APs"/>
Comments	<input type="text" value="Write a comment..."/> 0/255
Color	[Change]
Show in Address List	<input checked="" type="checkbox"/>
Members	<div><div> FortiAP1</div><div> FortiAP2</div></div>

Serial Number	<input type="text" value="FP221"/>
Name	<input type="text" value="FortiAP-1"/>
Comments	<input type="text" value="Write a comment..."/> 0/35
State	Authorized
Wireless Settings	
<input checked="" type="checkbox"/> Enable WiFi Radio	
SSID	<div><input checked="" type="radio"/> Automatically Inherit all SSIDs</div> <div><input type="radio"/> Select SSIDs</div>
Auto TX Power Control	<div><input checked="" type="radio"/> Disable <input type="radio"/> Enable</div>
TX Power	<div> <input type="range" value="100"/> 100 %</div>

Preauthorize FortiAP-2

Go to **WiFi & Switch Controller > Managed Devices > Managed FortiAP**.
Select **Create New**.

Enter the serial number of the FortiAP and give the Managed Access Point a name.

The FortiAP list will now show both FortiAP units. Since they are not currently connected, they will appear greyed out.

Apply the Custom AP profile

Go to **WiFi & Switch Controller > Managed Devices > Managed FortiAP**.

The same custom AP profile needs to be added to both the FortiAP units. Edit each one in turn.

Use the **[Change]** link to assign the custom AP profile.

Serial Number

FAP22B3

Name

FortiAP-2

Comments

Write a comment...0/35

State

Authorized

Wireless Settings

☒ Enable WiFi Radio

SSID

☒ Automatically Inherit all SSIDs

☐ Select SSIDs

Auto TX Power Control

☒ Disable

☐ Enable

TX Power

100 %

Mesh	Access Point	State	Connected Via	SSIDs	Channel
<input type="checkbox"/>	FortiAP-1	<input type="checkbox"/>	-	Radio 1: All Radio 2: All	Radio 1: 0 Radio 2: 0
<input type="checkbox"/>	FortiAP-2	<input type="checkbox"/>	-	Radio 1: All Radio 2: All	Radio 1: 0 Radio 2: 0

Serial Number

FP221B3X13019600

Name

FortiAP-1

Comments

Write a comment...0/35

Managed AP Status

Status

Online

Connected Via

Ethernet (192.168.11.2)

Base MAC Address

08:5b:0e:22:01:ae

Join Time

10/10/13 17:44

Clients

1

FortiAP OS Version

FP221B-v5.0-build048 [Upgrade]

State

Authorized

Deauthorize

Restart

Wireless Settings

AP Profile

FAP22xB-Mesh [Change]

The FortiAP list now shows that the SSIDs have been added to the appropriate radios on the APs.

Configure FortiAP-1 through its web interface

Certain parameters of the FortiAP units can only be configured by connecting to the unit directly, rather than through the FortiGate interface.

Reset the IP information of your computer to an address on the same subnet as the FortiAP. If the AP is in its factory default configuration, use the following address:

IP address: 192.168.1.100
Subnet mask: 255.255.255.0
Gateway: 192.168.1.1

Connect your computer to the FortiAP with an Ethernet cable. One end of the Ethernet cable connected to the network interface port of you computer and the other connected to the POE interface on the AP.

Access Point	State	Connected Via	SSIDs
FortiAP-1	✓	-	Radio 1: backhaul-ssid Radio 2: leaf-ssid
FortiAP-2	✓	-	Radio 1: backhaul-ssid Radio 2: leaf-ssid



Open a browser window and use the IP address of the FortiAP unit as the URL. The factory default IP address is *192.168.1.2*. Login with the name: *admin*. Password is null, so just press Login.



If this does not work, use the reset button to return the FortiAP to default settings.

Set **Address Mode** to **Static** and set **Local IP Address** to the same address as previously set on the FortiGate unit.

Set **Uplink** to **Ethernet** and **AC Discovery Type** to **Auto**.

Once the changes have been made, you will not be able to connect to the FortiAP unit through the web interface, because it is no longer on the same subnet as your computer.

Do not reset the IP configuration on the computer yet as you still need to configure FortiAP #2 and the same addresses will be used on both sides of the Ethernet connection.

Configure AP-2 through its web interface

As with the AP-1, connect to the web interface. Make sure to use the correct Ethernet port.

Network Configuration

Address Mode	<input checked="" type="radio"/> Static <input type="radio"/> DHCP
Management VLAN ID	<input type="text" value="0"/>
Local IP Address	<input type="text" value="192.168.11.2"/>
Local Network Mask	<input type="text" value="255.255.255.0"/>
Gateway IP	<input type="text" value="192.168.11.1"/>
Administrative Access	<input checked="" type="checkbox"/> HTTP <input type="checkbox"/> TELNET

Connectivity

Uplink	<input checked="" type="radio"/> Ethernet <input type="radio"/> Mesh <input type="radio"/> Ethernet with mesh backup support
--------	--

WTP Configuration

AC Discovery Type	<input checked="" type="radio"/> Auto <input type="radio"/> Static <input type="radio"/> DHCP <input type="radio"/> DNS <input type="radio"/> Broadcast <input type="radio"/> Multicast
AC Control Port	<input type="text" value="5246"/>
AC IP Address 1	<input type="text" value="192.168.1.1"/>



Set **Address Mode** to **Static** and set **Local IP Address** to the same address as previously set on the FortiGate unit.

Set **Uplink** is set to **Mesh**, the **AC Discover Type** to **Static**, and **AC IP Address 1** to the IP interface of the FortiGate port that is dedicated to the FortiAPs.

Reset the computer to its normal IP address configuration and login to the FortiGate unit.

Connect FortiAP-1 to the FortiGate interface dedicated to the FortiAPs (in the example, port 11).

Once the FortiAPs are configured and powered up, they should no longer be shown as online. The **Mesh** column will also show that FortiAP-2 is connected through a mesh to FortiAP-1.

Address Mode

☒ Static ☐ DHCP

Local IP Address

192.168.11.3

Local Network Mask

255.255.255.0

Gateway IP

192.168.11.1

Administrative Access

☒ HTTP ☐ TELNET

Uplink

☐ Ethernet ☒ Mesh ☐ Ethernet with mesh backup su

Mesh AP SSID

backhaul-ssid

Mesh AP Password

Ethernet Bridge

☐

AC Discovery Type

☐ Auto ☒ Static ☐ DHCP ☐ DNS ☐ Broadcast

AC Control Port

5246

AC IP Address 1

192.168.1.1

AC IP Address 2

AC IP Address 3

AC Data Channel Security

☐ Clear Text ☐ DTLS Enabled ☒ Clear Text or DTLS E

Mesh	Access Point	State	Connected Via	SSIDs	Channel	Clients
⌵	FortiAP-1	✔	📶 192.168.11.2	Radio 1: backhaul-ssid Radio 2: leaf-ssid	Radio 1: 40 Radio 2: 1	Radio 1: 1 Radio 2: 0
⌵	FortiAP-2	✔	🌐 192.168.11.3	Radio 1: backhaul-ssid Radio 2: leaf-ssid	Radio 1: 40 Radio 2: 6	Radio 1: 0 Radio 2: 1

(Alternative) Configure AP-2 through its console port

FortiAP-2 in the example is a FAP-220B. This model includes a console port. This allows for the option of using the CLI to configure the unit.

Instead of an Ethernet cable, use a console cable to connect from your computer to the console port of FortiAP #2. The exact details of connecting will defer slightly based on whether the console cable is connected directly from a serial port or through a USB adapter and what operating system is on your computer, but once the connection has been made it proceeds as follows:

Using a utility like Putty or Terminal, connect to the CLI. For more details on connecting read the Quick Start Guide for the model.

Login with the credentials:

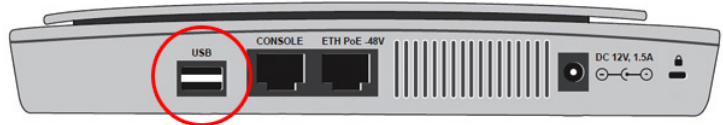
Username: admin

Password: <null>

Use the following commands to change the network configuration.

Change Address Mode to Static:

Set the IP address:



```
cfg -a ADDR_MODE=STATIC
cfg -c
```

```
cfg -a IPADDR=192.168.11.3
cfg -a AP_NETMASK:=255.255.255.0
cfg -a IPGW=192.168.11.1
cfg -c
```

Change Connectivity, remembering to choose a more secure password:

```
cfg -a MESH_AP_TYPE:=1
cfg -a MESH_AP_SSID:=backhaul-ssid
cfg -a MESH_AP_PASSWD:=12345678
cfg -c
```

Assign the discovery type to Static:

```
cfg -a AC_DISCOVERY_TYPE=1
cfg -c
```








Statically assign the IP address for the Access Controller (AC):

```
cfg -a AC_IPADDR=192.168.11.1
cfg -c
```

Creating security policies on the FortiGate

Go to **Policy > Policy > Policy** and create a policy to allow wireless users out to Internet

Set **Incoming Interface** to the leaf SSID, **Source Address** to the address for leaf channel users, **Outgoing Interface** to your Internet-facing interface, and **Enable NAT**.

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input checked="" type="radio"/> Address <input type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	leaf-ssid (SSID: leaf-ssid) 
Source Address	Leaf_Wireless_Subnet 
Outgoing Interface	wan1 
Destination Address	all 
Schedule	always 
Service	ALL 
Action	ACCEPT 
<input checked="" type="checkbox"/> Enable NAT	
<input checked="" type="radio"/> Use Destination Interface Address	<input type="checkbox"/> Fixed Port
<input type="radio"/> Use Dynamic IP Pool	
<input type="radio"/> Use Central NAT Table	
	<input type="text" value="Click to add..."/>

Create another policy to allow traffic to reach APs. This is primarily to allow access to the web interfaces of the FortiAPs, so if you wish you can limit the policy to only allow access to those IP addresses.

Set **Incoming Interface** to the internal network's interface (in the example, **LAN**), **Source Address** to the address for the internal network, **Outgoing Interface** to the port dedicated to the FortiAPs, and (optionally) **Destination Address** to the group containing both FortiAP addresses.



After policies are created, remember to place them at a proper point in the sequence so that they can be reached by the desired traffic but will not interfere with other traffic.

Results

Wireless devices are now able to connect to the leaf SSID, even if they are only within the range of FortiAP-2.

There are several ways to verify that the wireless network has been extended over both FortiAP units.

Go to **WiFi & Switch Controller > Managed Devices > Managed FortiAPs**.

You can see that **Radio 2** (leaf-ssid) on FortiAP-2 has one client connected to it, while the same SSID on FortiAP-1 does not.

Policy Type

Policy Subtype

Incoming Interface

Source Address

Outgoing Interface

Destination Address

Schedule

Service

Action

☐ Enable NAT

☒ Firewall ☐ VPN

☒ Address ☐ User Identity ☐ Device Identity

LAN

Internal_Network

port11 (FortiAP)

Mesh_APs

always

HTTP

ACCEPT

SSIDs	Channel	Clients
Radio 1: backhaul-ssid Radio 2: leaf-ssid	Radio 1: 40 Radio 2: 1	Radio 1: 1 Radio 2: 0
Radio 1: backhaul-ssid Radio 2: leaf-ssid	Radio 1: 40 Radio 2: 6	Radio 1: 0 Radio 2: 1


Go to **WiFi & Switch Controller > Monitor > Client Monitor**.



The client monitor which SSID and FortiAP that a client is connected to. In the example, a client has successfully connected to the leaf SSID on FortiAP-2.




Go to **WiFi & Switch Controller > Monitor > Wireless Health**.

For information on the leaf channel, which uses the 2.4 GHz frequency, view the **Top Client Count Per-AP (2.4 GHz Band)** widget. In the example, the only SSID on that frequency is for the leaf channel, so the client using radio 1 on FortiAP-2 must be using that SSID.

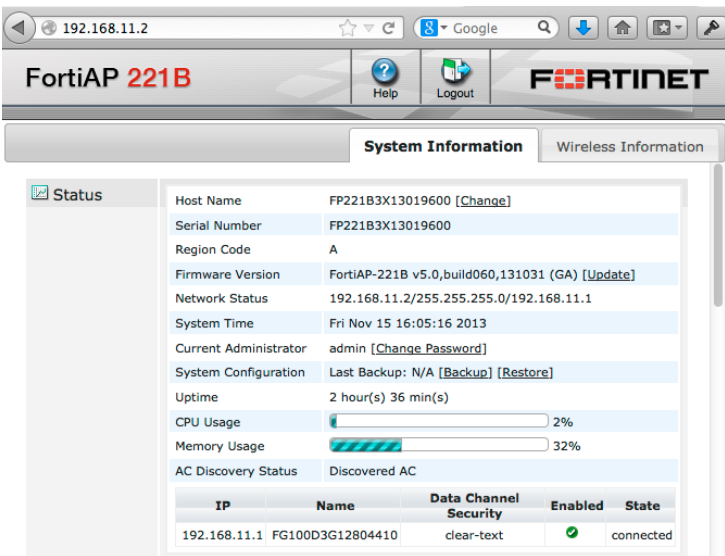
For information on the backhaul channel, which uses the 5 GHz frequency, view the **Top Client Count Per-AP (5 GHz Band)**. Again, in the example configuration, the only SSID on this frequency is for the backhaul channel.

SSID	FortiAP	User	IP	Device
leaf-ssid	FortiAP-2 (2)		192.168.205.5	 d8:30:62:9b:63:1b

Top Client Count Per-AP (2.4 GHz Band)			
FortiAP	Client Count	Channel	Bandwidth (Tx/Rx)
FortiAP-2 (2)	1 	6	925 bps 
FortiAP-1 (2)	0	1	340 bps 

Top Client Count Per-AP (5 GHz Band)			
FortiAP	Client Count	Channel	Bandwidth (Tx/Rx)
FortiAP-1 (1)	1 	40	3.28 Kbps 
FortiAP-2 (1)	0	40	1018 bps 

Open a browser and verify that you can connect to the web interface of FortiAP-1, using the IP set in the configuration (in the example, *http://192.168.11.2*).



Connect to the web interface of FortiAP-2 using its assigned IP (in the example, *http://192.168.11.3*).

